Amendments to the Claims

1. (currently amended) A packet processing method comprising:

receiving a plurality of packets;

receiving a security association handle for each packet in the plurality of packets, wherein the security association handle includes a set of selectors;

for each packet, identifying a flow entry for the packet, including:

determining a flow element address for the packet,

retrieving a first flow element using the flow element address, wherein the first flow element includes a plurality of flow entries,

determining whether a selector in the set of security association handle selectors is present in one of the plurality of flow entries, and

retrieving a second flow element if a selector in the set of security association handle selectors is not present in one of the plurality of flow entries;

retrieving security association information for each packet using the identified flow entry;

generating header information for each of the plurality of packets;

adding the header information to each of the plurality of packets to generate encapsulated packets; and

distributing the encapsulated packets to a plurality of ~~encryption~~ cryptographic processors.

2. (original) The method of claim 1 wherein the information comprises one or more of the group consisting of sequence number and byte count.

3. (original) The method of claim 1 wherein the encapsulated packets comprise IPsec packets.

4. (original) The method of claim 1 wherein packets are encapsulated on a per-packet basis.

5. (canceled).

6. (original) The method of claim 1 wherein the packets are received from a host processor.

7-13. (canceled)

14. (currently amended) A packet processing method comprising:

receiving a plurality of ~~encrypted~~ packets comprising header information and encrypted data;

receiving a security association handle for each packet in the plurality of packets, wherein the security association handle includes a set of selectors;

for each packet, identifying a flow entry for the packet, including:

determining a flow element address for the packet,

retrieving a first flow element using the flow element address, wherein the first flow element includes a plurality of flow entries,

determining whether a selector in the set of security association handle selectors is present in one of the plurality of flow entries, and

retrieving a second flow element if a selector in the set of security association handle selectors is not present in one of the plurality of flow entries;

retrieving security association information for each packet using the identified flow entry;

distributing the ~~encrypted~~ packets to a plurality of ~~decryption~~ cryptographic processors;

decrypting the encrypted portion of each packet based on a portion of the security association information retrieved for the packet;

modifying, by a common processing component, at least a portion of the header information of the decrypted packets; and

transmitting the decrypted packets.

15. (original) The method of claim 14 wherein the at least a portion of the header information comprises one or more of the group consisting of sequence number and byte count.

16. (original) The method of claim 14 wherein the encrypted packets comprise IPsec packets.

17. (original) The method of claim 14 wherein the at least a portion of the header information is modified on a per-packet basis.

18. (canceled).

19. (original) The method of claim 14 wherein the packets are transmitted to a host processor

20 - 27. (canceled)

28. (currently amended) A packet processing system comprising:

at least one media access controller for receiving a plurality of packets;

at least one data memory for storing security association information;

~~a header processor for modifying at least a portion of the security association information and adding header information to the packets to generate encapsulated packets, wherein the header information comprises the modified at least a portion of the security association information;~~ and

a cryptographic processing module, wherein the cryptographic processing module includes:

a policy lookup unit configured to identify a flow associated with each of the received plurality of packets and to retrieve a security association for each identified flow;

a merge data unit coupled to the policy lookup unit configured to merge a portion of the security association retrieved by the policy lookup unit with the associated packet,

a plurality of ~~encryption~~ cryptographic processors, each coupled to the merge data unit for ~~encrypting~~ performing cryptographic operations on the ~~encapsulated~~ merged packets.

29. (original) The packet processing system of claim 28 wherein the at least a portion of the security association information comprises one or more of the group consisting of sequence number and byte count

30-31. (canceled)

32. (new) The method of claim 1, wherein determining a flow element address includes:

hashing the selectors in the set of security association handle selectors to generate the flow element address.

33. (new) The method of claim 1, wherein the step of determining a flow element address includes:

retrieving a security parameter index from the set of security association handle selectors; and

using the retrieved security parameter index as the flow element address.

34. (new) The method of claim 1, further comprising:

processing each encapsulated packet based on the retrieved security association information for the packet; and

transmitting the processed packet.

35. (new) The method of claim 1, further comprising:

modifying a least a portion of the retrieved security association information; and

generating header information for the packets including a portion of the modified security association information.

36. (new) The method of claim 14, wherein determining a flow element address includes:

hashing the selectors in the set of security association handle selectors to generate the flow element address.

37. (new) The method of claim 14, wherein the step of determining a flow element address includes:

retrieving a security parameter index from the set of security association handle selectors; and

using the retrieved security parameter index as the flow element address.

38. (new) The packet processing system of claim 28, wherein the cryptographic processing module further comprises:

a distributor coupled between the merge data unit and the plurality cryptographic processors for distributing merged packets to the plurality of cryptographic processors.

39. (new) A method for determining security association information in a cryptographic processor comprising:

receiving a security association handle for a packet, wherein the security association handle includes a set of selectors;

determining a flow element address for the packet;

retrieving a first flow element using the flow element address, wherein the first flow element includes a plurality of flow entries;

identifying a flow entry having a selector matching a selector in the set of security association handle selectors;

retrieving security association information using the identified flow entry; and

transmitting at least a portion of the retrieved security association information to a cryptographic processing engine.

40. (new) The method of claim 39, further comprising:

retrieving a second flow element if a selector in the set of security association handle selectors is not present in one of the plurality of flow entries

41. (new) The method of claim 39, wherein determining a flow element address includes:

hashing the selectors in the set of security association handle selectors to generate the flow element address.

42. (new) The method of claim 39, wherein the step of determining a flow element address includes:

retrieving a security parameter index from the set of security association handle selectors; and

using the retrieved security parameter index as the flow element address.